DATA PROCESSING APPARATUS, METHOD THEREOF, PROGRAM THEREOF, LINEAR CONVERSION CIRCUIT AND ENCRYPTION CIRCUIT

ABSTRACT

A data processing method for specifying linear conversion for making the number of active S-box maximum, wherein a plurality of linear conversion candidates satisfying a restriction on a circuit for realizing linear conversion candidates are specified among the plurality of linear conversion candidates, linear conversion processing is performed based on a plurality of input data on each of the specified linear conversion candidates, a minimum value of the number of zeros arisen in processing results thereof (a so-called active S-box) is obtained, a linear conversion candidate making the minimum value largest is specified, and a linear conversion portion is configured based on the specified linear conversion candidate.